AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently amended) A method for managing a database system, comprising:

receiving a command to perform an administrative function involving an object defined within the database system;

determining if the object is a sensitive object that is associated with security functions in the database system, wherein the sensitive object and only the sensitive object is encrypted in the database system, wherein the sensitive object can include a sensitive row within a table in the database system, wherein the sensitive row contains sensitive data, and wherein other rows in the table need not contain sensitive data;

wherein the sensitive object can include one of:

a sensitive table containing sensitive data in the database system, and

an object that represents a sensitive user of the database system who is empowered to access sensitive data,

whereby an administrator cannot become a sensitive user and thereby obtain access to sensitive objects indirectly;

if the object is not a sensitive object, and if the command is received from a normal database administrator for the database system, allowing the administrative function to proceed; and

if the object is a sensitive object, and if the command is received from a normal system administrator, disallowing the administrative function.

2. (Original) The method of claim 1, further comprising:

receiving a request to perform an operation on a data item in the database system;

if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, allowing the operation to proceed if the sensitive user has access rights to the data item; and

if the data item is a sensitive data item and the request is received from a normal user, disallowing the operation.

3. (Original) The method of claim 2, wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the method further comprises decrypting the data item using an encryption key after the data item is retrieved.

4. (Original) The method of claim 3, wherein the encryption key is stored along with a table containing the data item.

5. (Original) The method of claim 4, wherein the encryption key is stored in encrypted form.

6. (Canceled).

7. (Original) The method of claim 1, wherein if the object is not a sensitive object, and if the command to perform the administrative function is received from a security officer, the method further comprises allowing the security officer to perform the administrative function on the object.

8. (Original) The method of claim 1,

wherein the database system includes a number of sensitive data items; and

wherein only specific sensitive users are allowed to access a given sensitive data item.

9. (Currently amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for managing a database system, the method comprising:

receiving a command to perform an administrative function involving an object defined within the database system;

determining if the object is a sensitive object that is associated with security functions in the database system, wherein the sensitive object and only the sensitive object is encrypted in the database system, wherein the sensitive object can include a sensitive row within a table in the database system, wherein the sensitive row contains sensitive data, and wherein other rows in the table need not contain sensitive data;

wherein the sensitive object can include one of:

a sensitive table containing sensitive data in the database system, and

an object that represents a sensitive user of the database system who is empowered to access sensitive data,

whereby an administrator cannot become a sensitive user and thereby obtain access to sensitive objects indirectly;

if the object is not a sensitive object, and if the command is received from a normal database administrator for the database system, allowing the administrative function to proceed; and if the object is a sensitive object, and if the command is received from a normal system administrator, disallowing the administrative function.

10. (Original) The computer-readable storage medium of claim 9, wherein the method further comprises:

receiving a request to perform an operation on a data item in the database system;

if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, allowing the operation to proceed if the sensitive user has access rights to the data item; and

if the data item is a sensitive data item and the request is received from a normal user, disallowing the operation.

11. (Original) The computer-readable storage medium of claim 10, wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the method further comprises decrypting the data item using an encryption key after the data item is retrieved.

12. (Original) The computer-readable storage medium of claim 11, wherein the encryption key is stored along with a table containing the data item.

13. (Original) The computer-readable storage medium of claim 12, wherein the encryption key is stored in encrypted form.

14. (Canceled).

15. (Original) The computer-readable storage medium of claim 9, wherein if the object is not a sensitive object, and if the command to perform the administrative function is received from a security officer, the method further comprises allowing the security officer to perform the administrative function.

16. (Original) The computer-readable storage medium of claim 9,

wherein the database system includes a number of sensitive data items; and

wherein only specific sensitive users are allowed to access a given sensitive data item.

17. (Currently amended) An apparatus for managing a database system, comprising:

a command receiving mechanism that is configured to receive a command to perform an administrative function involving an object defined within the database system;

an execution mechanism that is configured to,

determine if the object is a sensitive object that is associated with security functions in the database system, wherein the sensitive object and only the sensitive object is encrypted in the database system, wherein the sensitive object can include a sensitive row within a table in the database system, wherein the sensitive row contains sensitive data, and wherein other rows in the table need not contain sensitive data, wherein the sensitive object can include one of:

a sensitive table containing sensitive data in the database system, and an object that represents a sensitive user of the database system who is empowered to access sensitive data,

whereby an administrator cannot become a sensitive user and thereby obtain access to sensitive objects indirectly;

allow the administrative function to proceed, if the object is not a sensitive object, and if the command is received from a normal database administrator for the database system, and to

disallow the administrative function, if the object is a sensitive object, and if the command is received from a normal system administrator.

18. (Original) The apparatus of claim 17,

wherein the command receiving mechanism is configured to receive a request to perform an operation on a data item in the database system;

wherein the execution mechanism is configured to,

allow the operation to proceed, if the data item is a sensitive data item, if the request is received from a sensitive user who is empowered to access sensitive data, and if the sensitive user has access rights to the data item, and to

disallow the operation, if the data item is a sensitive data item, and if the request is received from a normal user.

19. (Original) The apparatus of claim 18, further comprising a decryption mechanism, wherein if the data item is a sensitive data item, if the operation is allowed to proceed, and if the operation involves retrieval of the data item, the

decryption mechanism is configured to decrypt the data item using an encryption key after the data item is retrieved

20. (Original) The apparatus of claim 19, wherein the encryption key is stored along with a table containing the data item.

21. (Original) The apparatus of claim 20, wherein the encryption key is stored in encrypted form.

22. (Canceled).

23. (Original) The apparatus of claim 17, wherein if the object is not a sensitive object, and if the command to perform the administrative function is received from a security officer, the execution mechanism is configured to allow the security officer to perform the administrative function.

24. (Original) The apparatus of claim 17,

wherein the database system includes a number of sensitive data items; and

wherein only specific sensitive users are allowed to access a given sensitive data item.